APRIL/MAY 2025

FECA63B/FECS63B/CECA63B/ CECS63B — CRYPTOGRAPHY

Time : Three hours Maximum : 75 marks

SECTION A — (10 × 2 = 20 marks)

Answer ALL questions.

Shanmuga Industries Arts & Science College T.V.Malai

1. Name any two Security Services.
2. What is Data Confidentiality?
3. Differentiate a Block Cipher and a Stream Cipher.
4. List the five modes of operations of Block Cipher.
5. What is an Elliptic Curve?
6. State the difference between Private Key and Public Key algorithm.
7. Write the role of compression function in hash function.

8. Specify the various types of authentication protocol.

9. Name the cryptographic keys used in PGP.

10. What are the roles of Firewalls.

SECTION B — (5 × 5 = 25 marks)

Answer ALL questions.

11. (a) Explain the model for Network Security.

Or

(b) Write a detailed note on Security attacks.

12. (a) What is Steganography ? Explain.

Or

(b) Explain DES encryption algorithm in detail.

13. (a) What are the applications of Public Key Crypto Systems? Discuss.

Or

(b) Describe the Diffie-Hellman Key Exchange mechanism.

Shanmuga Industries Arts & Science College T.V.Malai

14. (a) Explain Message Authentication Requirements.

Or

(b) Describe the basics of Digital Signature.

15. (a) What is MIME? List the five header fields defined in MIME.

Or

(b) List and define three classes of Intruders.

SECTION C — (3 × 10 = 30 marks)

Answer any THREE questions.

16. Explain the OSI security architecture model with neat diagram.

17. Write a detailed note on Block Cipher design principles.

18. Elaborate on Elliptic Curve Cryptography.

19. Illustrate the Secure Hash Algorithm.

20. Describe the various types of Firewalls.